(Attach C)

State of Iowa Data Center Standard

November 12, 2009

Purpose:

To provide a data center standard that protects critical computing infrastructure from risks associated with loss of power, fire, unmanaged temperature, or unauthorized access.

Overview:

This standard is intended to apply to all State of Iowa data centers as defined below. The intent of this standard is to reduce risk and increase the longevity of critical network assets.

Several Iowa agency network engineers conducted research and toured both government and private data centers to provide state agencies with the following data center standard practices and best practices.

Scope:

For the purpose of this standard, all State of Iowa participating agencies, boards or commissions operating a data center facility will ensure the proper management, risk mitigation, redundancy, and reliability of the following data center areas:

- Power
- Physical Security
- HVAC
- Fire Suppression
- Cable Management

Agencies will be required to comply with the provisions as stated in the standard practice section of this standard no later than June 30, 2010. The Technology Governance Board TGB has the authority to determine entity compliance or non-compliance of this standard. Failure to comply with this standard will result in a review by the TGB.

Updates:

This document will be reviewed at least every two years and updated as needed.

Definitions:

Selected terms used in the Data Center Standard are defined below:

- **Agency -** means any agency as listed in Iowa Code Chapter 8A Section 201 paragraph 4.
- **Best Practice –** is a technique, method, process, or activity that is believed to be effective at delivering a particular outcome. Best practices noted in this document are viewed as recommendations, not requirements.
- **Critical IT infrastructure –** is defined by business service restoration within 72 hours in an agency's disaster recovery plan.

- **Data Center –** is a facility dedicated to the purpose of securing data and systems and is used to house network server systems and associated components. It includes networked servers, controlled access, environmental controls such as air conditioning and fire suppression, power and electrical systems, and networking equipment. The threshold of what facilities is considered to be a data center is provided below:

Space Type	Typical Site Infrastructure System Characteristics
Localized data center	*Typically use under-floor or overhead air distribution systems and a few in-room computer room air conditioner (CRAC) units. CRAC units in localized data centers are more likely to be air cooled and have constant-speed fans and are thus relatively low efficiency. Operational staff is likely to be minimal, which makes it likely that equipment orientation and airflow management are not optimized. Air temperature and humidity are tightly monitored. However, power and cooling redundancy reduce overall system efficiency.*
Mid-tier data center	*Typically use under-floor air distribution and in-room CRAC units. The larger size of the center relative to those listed above increases the probability that efficient cooling, e.g., a central chilled water plant and external storage central air handling units with variable speed fans, is used. Staff at this size data center may be aware of equipment orientation and airflow management best practices. However, power and cooling redundancy may reduce overall system efficiency.*
Enterprise-class data center	*The most efficient equipment is expected to be found in these large data centers. Along with efficient center cooling, these data centers may have energy management systems. Equipment orientation and extensive airflow management best practices are most likely external storage implemented. However, enterprise-class data centers are designed with maximum redundancy, which can reduce the benefits, gained from the operational and technological efficiency measures.*

- **Environmental Stability –** refers to the controls for fire suppression, temperature, humidity, and air quality.
- **Networking and data cabling –** terminology pertaining to the installation and maintenance of twisted-pair and optical fiber cabling.
- **Physical Security –** describes both measures that prevent or deter attackers from accessing a facility, resource, or information stored on physical media and guidance on how to design structures to resist various hostile acts.
- **Power and Electrical Systems –** terminology relating to reliable, conditioned power that is provided for computer and networking systems located within a data center.
- **Standard Practice –** is a technique, method, process, or activity that is believed to be effective at delivering a particular outcome. Standard practices noted in this document are viewed as requirements, not recommendations.
- **Visitor** – Any non-authorized state personnel, non-authorized vendors, or the general public using or touring State of Iowa facilities.

Data Center Standard Practices:

State of Iowa data center *standard practices* require that:

1. The following physical security practices be implemented:
    a. Barriers shall exist that restrict access to data center rooms;
    b. Physical access shall be restricted to selected personnel, with an auditable physical security process using security card access. If a security card system is

not present, room(s) shall be secured by key or keypad system. A key system shall have an audited checkout process;

c. Access shall be restricted to employees and vendors who need to maintain equipment or infrastructure in the room(s). An escort is required for all visitors and vendors to the room(s). In addition, visitors and vendors shall be given a physical access token (badge or access device) that identifies visitors as non-employee(s);
d. Whenever practical, critical IT infrastructure as designated by the agency director in consultation with the State CIO, should reside inside data centers. It is not the intent to apply this standard to non-critical servers, network infrastructure or communication assets located inside of unimproved utility closets;
e. If the site is subject to Payment Card Industry (PCI) rules and requirements, video cameras shall be used to monitor sensitive areas. Recorded video shall be retained for a minimum of three months.

2. The following environmental stability practices be implemented:
    a. Smoke detectors and sprinkler systems or clean agent fire suppression gaseous systems are required;
    b. Monitoring, alarming and alerting shall be in effect in case fire and all fire suppression systems must be installed and maintained in accordance with local fire code;
    c. Air handling equipment must supply sufficient cooling and humidity controls to meet the most restrictive equipment cooling and humidity specifications of the equipment residing within the data center;
    d. Storage of flammable or combustible materials (e.g. wood, cardboard and corrugated paper, plastic or foam packing materials, flammable liquids or solvents) shall not be allowed in the room(s).

3. The following power and electrical system practices be implemented:
    a. All devices, including servers, networking equipment, etc., shall be protected by conditioned power and suitable UPS sufficient to maintain power until power is restored through commercial power or generator backup;
    b. Cabinets and racks shall be properly grounded, in accordance with existing commercial building grounding and bonding standards.

4. The following networking and data cabling practices be implemented:
    a. Data cabling shall be installed and tested in accordance with industry standards and best practices listed in the ANSI/TIA-568 family of Telecommunications Standards;
    b. Data cabling routed outside of cabinets shall be protected and contained, using solutions such as cable trays, flexible conduit, J-hooks, etc.;
    c. Data cabling routed within or between bayed cabinets shall be done in a manner so as to not inhibit air flow through the cabinet. Cabling within a cabinet shall be dressed in such a way as to enhance air flow through the cabinet;
    d. Twisted-pair and fiber panels shall be labeled, and all cables shall be labeled at both ends, including twisted-pair and fiber patch cords;
    e. Cabling, cable lengths, and terminations shall meet current BICSI cabling and termination standards.

5. Waivers to the standard may be granted using current Iowa Administrative Code Chapter 25, Section 11-25.6 (8A).

Data Center Best Practices:

State of Iowa data center *best practices* recommend that:

1. The following physical security practices be implemented:
    a. Video camera surveillance and security escorts should be considered in cases where large data centers contain sensitive information;
    b. Gates or gate-like systems should be used above dropped ceilings and below raised floors to deny access into false floor/ceiling space;
    c. Biometric identification systems and processes are recommended for access to highly sensitive areas of a data center;
    d. Where possible, mantraps should be established to segment areas of the data center, with location-based access only;
    e. Limit or avoid windows in the room(s);
    f. Food and drink should not be allowed.
2. The following environmental stability practices be implemented:
    a. Redundant cooling is recommended. N+1 or outside air should augment cooling systems. Use of outside air should be considered to help economize cooling;
    b. A clean agent fire-suppression system such as FM-200 is recommended, where possible;
    c. Monitoring, alarming, and alerting should be in effect for instances of temperature and humidity thresholds and failures;
    d. Monitoring, alarming, and alerting are recommended for water detection;
    e. Blanking panels should be placed in cabinets to help direct air flow through rack-mounted devices;
    f. Temperature and humidity range requirements should be measured at multiple entry points on equipment racks, and at the ventilation output ducts.
3. The following power and electrical system practices be implemented:
    a. Power availability should be 100 percent and should guide decision making on UPS and power distribution;
    b. Monitoring, alarming, and alerting should be in effect for instances of UPS thresholds and failures, and power or breaker failures;
    c. Room-level PDUs should be protected by room UPS;
    d. Cabinet-level PDUs should be protected either by room or cabinet UPS;
4. The following networking and data cabling practices be implemented:
    a. Data cabling installers should make a best effort to maintain neat and easily identifiable cabling systems, in order to support debugging and documentation efforts;
    b. Data cabling exterior to a cabinet should be routed through overhead cable trays, where possible, and twisted-pair and fiber cabling should be segregated within such trays;
    c. Data cabling installers should test all new, installed cables, and test results should be provided to the customer in electronic form.

Appendix A. Data Center Facility Definitions

Data Center Typical IT Equipment and Site Infrastructure System Characteristics, by Space Type

Space Type	Typical Site Infrastructure System Characteristics
Server closet[a]	*Typically conditioned through an office HVAC system. To support VOIP and wireless applications, UPS and DC power systems are sometimes included in server closets. Environmental conditions are not as tightly maintained as for other data center types. HVAC energy efficiency associated with server closets is probably similar to the efficiency of office HVAC.*
Server room[a]	*Typically conditioned through an office HVAC system, with additional cooling capacity, probably in the form of a split system specifically designed to condition the room. The cooling system and UPS equipment are typically of average or low efficiency because there is no economy of scale to make efficient systems more cost competitive.*
Localized data center[b]	*Typically use under-floor or overhead air distribution systems and a few in-room computer room air conditioner (CRAC) units. CRAC units in localized data centers are more likely to be air cooled and have constant-speed fans and are thus relatively low efficiency. Operational staff is likely to be minimal, which makes it likely that equipment orientation and airflow management are not optimized. Air temperature and humidity are tightly monitored. However, power and cooling redundancy reduce overall system efficiency.*
Mid-tier data center[b]	*Typically use under-floor air distribution and in-room CRAC units. The larger size of the center relative to those listed above increases the probability that efficient cooling, e.g., a central chilled water plant and external storage central air handling units with variable speed fans, is used. Staff at this size data center may be aware of equipment orientation and airflow management best practices. However, power and cooling redundancy may reduce overall system efficiency.*
Enterprise-class data center[b]	*The most efficient equipment is expected to be found in these large data centers. Along with efficient center cooling, these data centers may have energy management systems. Equipment orientation and extensive airflow management best practices are most likely external storage implemented. However, enterprise-class data centers are designed with maximum redundancy, which can reduce the benefits gained from the operational and technological efficiency measures.*

[a] Note: Does not meet the definition of a data center.
[b] Note: Meets the definition of a data center.

(U.S. Environmental Protection Agency, 2007)